**PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| In re application of: | |
| Hinchliffe et al. | Art Unit: 2143 |
| Application No. 10/028,412 | Examiner: Dennison, Jerry B. |
| Filed: 12/21/2001 | Atty. Docket No. NAI1P344/01.249.01 |
| For: DESKTOP SECURITY IN PEER-TO-PEER NETWORKS | Date: 09/27/2007 |

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences**

**REPLY BRIEF (37 C.F.R. § 41.37)**

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 08/27/2007.

Following is an issue-by-issue reply to the Examiner's Answer.

Issue #1:

The Examiner has rejected Claims 1, 15, 29, 45 and 48 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

*Group #1: Claims 1, 15 and 29*

The Examiner has stated that it is unclear to the Examiner what "and operate substantially" means. The Examiner has also stated that it is unclear as to what is required by the server and that using the server for anything is an option. However, appellant respectfully asserts that the claim language in the foregoing claims expressly requires that "the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network" (emphasis added). Thus, the peers, at most, use the server for providing addresses for the peers in the peer-to-peer network.

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that 'the term "substantially" in Claims 1, 15, and 29 is a relative term that renders the claim indefinite.' In addition, the Examiner has argued that "[t]he limitation refers to a peer in a peer-to-peer network to operate substantially" and that '[i]t is unclear to the Examiner as to what degree "substantially" is referring.' Appellant respectfully disagrees with such arguments, and offers the following exemplary definition as illustrative evidence of the plain and ordinary meaning of such term, insofar as it is not inconsistent with the originally filed specification:

**substantially**
adv.

Considerable in importance, value, degree, amount, or extent

*Source: The American Heritage® Dictionary of the English Language, Fourth Edition*

The Examiner is reminded that the term "substantially" is often used in conjunction with another term to describe a particular characteristic of the claimed invention. It is a broad term. *In re Nehrenberg*, 280 F.2d 161, 126 USPQ 383 (CCPA 1960). Further, the court held that the limitation "to substantially increase the efficiency of the compound as a copper extractant" was definite in view of the general guidelines contained in the specification. *In re Mattison*, 509 F.2d 563, 184 USPQ 484 (CCPA 1975). Similar to *In re Mattison*, the current specification introduces peer-to-peer networks in paragraph [0003] of page 2, which provides analogous guidelines as to what "substantially" refers in the context of the claimed "substantially without a server." More importantly, appellant's claims what is meant by "substantially," by requiring that "peers ... connect and operate *substantially without a server* **by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network**" (emphasis added). The claimed term "substantially" is thus deemed definite.

Still yet, the court held that the limitation "which produces substantially equal E and H plane illumination patterns" was definite because one of ordinary skill in the art would know what was meant by "substantially equal." *Andrew Corp. v. Gabriel Electronics*, 847 F.2d 819, 6 USPQ2d 2010 (Fed. Cir. 1988). It is similarly argued that, in the case of the presently claimed invention, one of ordinary skill would know what is meant by the claimed "peer-to-peer network [that] permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network," since such claim language clearly defines what is well known to be a peer-to-peer network.

In addition, the Examiner has argued that 'the limitation recites operating without the server, and then the limitation recites, "by utilizing the server".' The Examiner continued, arguing that "[t]he limitation contradicts itself by reciting **not using the server to connect and operate substantially**, and then reciting **using the server to connect and operate substantially**." Appellant respectfully disagrees with the Examiner's argument and asserts that the claims require that "the peer-to-peer network permits peers to **connect and operate** *substantially* without a server" and then continue with more specificity by requiring that the server is utilized "**at most, for providing addresses for the peers in the peer-to-peer network**" (emphasis added), as claimed by appellant. Thus, such phrases are not contradictory, since the latter phrase simply calls out what is meant by "connect[ing] and operat[ing] *substantially* **without** a server." If the

term "substantially" were to be omitted, the Examiner's arguments would be persuasive. However, this is not the case.

In addition, appellant respectfully disagrees with the Examiner's assertion that "at most" means it is not a requirement. The term "at most" refers to that fact that the server does not do more than "provid[e] addresses for the peers in the peer-to-peer network" (emphasis added), as claimed by appellant.

It is finally noted with respect to this issue that the above claim language was entered to specifically counter the Examiner's broadened interpretation of a peer-to-peer network to encompass client/sever frameworks. Such claim language clearly distinguishes the claimed peer-to-peer network from client/server frameworks.

*Group #2: Claim 45*

The Examiner has stated that it is unclear what the claim language means. Particularly, the Examiner queries "what action is taken." Appellant further asserts that the actual action taken is not claimed and would unduly limit such claim.

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that 'the phrase "takes action" is unclear as to what is required by the claim' and that "it is unclear to Examiner as to what is actually being performed in the claim." Appellant respectfully asserts that the claimed "share configuration loop ... "take[s] action as a function of a type of the changes" (emphasis added). Again, appellant further asserts that a specific action taken is not claimed and would unduly limit such claim. Appellant believes that the current rejection should be withdrawn for reasons similar to those that the Examiner withdrew the rejection of Claim 48 below.

*Group #3: Claim 48*

The Examiner has stated that it is unclear why the configuration loop examines against a previously recorded share configuration. Appellant respectfully asserts that claiming a reason why "the share configuration loop examines a current share configuration against a previously

recorded shared configuration" would unduly limit such claim by limiting the function to a claimed purpose.

In the Examiner's Answer dated 08/27/2007, the Examiner "submit[ed] that [appellant's] argument is persuasive and the rejection has been withdrawn."

Issue #2:

The Examiner has rejected Claims 1, 2, 5, 11, 15, 16, 19, 25, 29, 30, 33, 39 and 45-49 under 35 U.S.C. 103(a) as being unpatentable over Welch, Jr. et al., U.S. Patent No. 5,862,335, in view of Meadway et al., U.S. Patent No. 6,675,205.

*Group #1: Claims 1, 2, 15, 16, 29 and 30*

It is noted that the Examiner has attempted to interpret appellant's claimed peer-to-peer network to refer to, for example, any client and server communications. Appellant respectfully disagrees with this interpretation, especially in view of the previous amendments which require that "the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network."

The Examiner has relied on the following excerpts from Meadway to make a prior art showing of appellant's claimed "performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network" (see this or similar, but not identical language in each of the foregoing claims).

> "Expanding on the above concepts, the invented system is a service which performs centralized searches based on index information transmitted by peer systems to the central site using an agent program running on each peer, and **then directs the peer systems to each other for the purpose of retrieving files.**" (Col. 1, lines 45-52-emphasis added)

> "...the file is sent by the system containing the file either to the central site or directly to the user who requested the file via email attachment." (Col. 1, lines 63-65)

> "agent program downloaded and installed by each peer system user. This agent program is described in detail in pending U.S. patent application Ser. Nos. 09/419,405, U.S. Pat. No. 6,516,337, and 09/575,971, filed May 23, 2000, by the same inventors which are hereby incorporated by reference. The indexing process on each system may be initiated manually or on a scheduled basis, with updates transmitted whenever the user connects to the central service." (Col. 2, lines 1-10)

Appellant respectfully asserts that the excerpts relied on by the Examiner simply relate to "direct[ing] the peer systems to each other for the purpose of retrieving files" (see emphasized excerpt above). In no way do such excerpts teach appellant's specific claim language, namely "performing an action associated with a particular pattern when the particular pattern is detected..." (emphasis added), especially when read in the context of the remaining claim language where "suspicious activity [is monitored] based on [the] patterns of activity" (emphasis added). Clearly, only generally directing peer systems to each other, as in Meadway, does not meet "performing an action associated with a particular pattern" where such monitoring is with respect to "suspicious activity," in the context claimed by appellant.

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that appellant's claimed "performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network" discloses, in the broadest reasonable interpretation, "[i]f something occurs, do something." Appellant respectfully disagrees, and asserts that appellant claims that if a "particular pattern is detected in the peer-to-peer network" then "[perform] an action associated with a particular pattern" (emphasis added).

Further, the Examiner has argued that "Meadway disclosed when the central server receives an updated version of the client's index of shared data on a scheduled basis (Meadway, col. 2, lines 5-7); the central server performs updating the central server's local index (Meadway, col. 4, lines 18-25)." In addition, the Examiner asserts that "[a] particular pattern of activity is the client sending updated versions of the client's index on a scheduled basis." However, Meadway discloses "[t]he indexing process on each system may be initiated manually or on a scheduled basis, with updates transmitted **whenever** the user connects to the central service" (emphasis added). Clearly, sending updates whenever the user connects fails to disclose any sort of "pattern of activity," as claimed by appellant.

In addition, the Examiner has argued that "Welch disclosed if the AME identifies a packet as being part of an existing file transfer, the AME updates the appropriate record in the database, the detected pattern being that the packet is part of an existing file request **114**, and the performed action being updating the appropriate record in the database **120** (Welch, col. 6, lines 21-30, Fig. 5, 114, 120)." Appellant respectfully asserts that merely "identify[ing] that packet as part of an existing file transfer AME 81 branches to step 120" fails to even suggest that a "particular pattern is detected in the peer-to-peer network" (emphasis added), as claimed by appellant.

The Examiner has also relied on the above cited excerpts to make a prior art showing of appellant's claimed technique "wherein a pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data." Appellant respectfully asserts that nowhere in the above excerpts is there even any mention of defining the pattern of activity "in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data," as claimed by appellant (emphasis added).

Instead, Meadway simply teaches that "index information [is] transmitted by peer systems to the central site using an agent program running on each peer, and then...the peer systems [are directed] to each other for the purpose of retrieving files" (see excerpts above). Appellant notes that such indexed information relates to the "contents of the files" (see Col. 2, line15), and therefore, no baseline of authorized shares and permissions is established in Meadway, in the context claimed by appellant.

The Examiner has again relied on the above cited excerpts to make a prior art showing of appellant's claimed technique "wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline." Appellant asserts that such excerpts yet again fail to teach "evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline," as claimed by appellant (emphasis added). In the excerpts above, Meadway discloses that "updates [are] transmitted whenever the user

connects to the central service." However, such updates relate to the indexing process, as disclosed in the excerpts above, and not "evaluating a change...with respect to the baseline" where such baseline is of "authorized shares and permissions in association with the shared data," as claimed by appellant.

In the Examiner's Answer dated 08/27/2007, the Examiner stated that "Meadway disclosed that the central server receives an updated version of the client's index of shared data on a scheduled basis (Meadway, col. 2, lines 5-7)." Appellant respectfully asserts that Meadway discloses that "[t]he indexing process on each system may be initiated manually or on a scheduled basis, with updates transmitted whenever the user connects to the central service" (emphasis added). Clearly, Meadway discloses that the indexing process may be initiated manually or on a scheduled basis, not that the updates are transmitted on a scheduled basis as asserted by the Examiner. In contrast to the Examiner's arguments, Meadway discloses that updates are transmitted whenever the user connects to the central service. Further, the Examiner has argued that "the pattern of activity is the index of shared data at the peer." Clearly, Meadway's disclosure of an "indexing process on each system" fails to even suggest a technique "wherein a pattern of activity is defined in terms of a configuration of shared data on a peer" (emphasis added), as claimed by appellant.

Further, the Examiner has argued that "[o]ne of ordinary skill in the art would interpret peers selecting which files they want to share with the network as authorizing or permitting which files are shared with other peers on the network." Appellant asserts that Meadway discloses that "[t]he agent reports to the central server the identities of files on the computer that will be provided if requested by others" (emphasis added). Simply teaching to report the identities of files that will be provided if requested fails to even suggest a "configuration establishing a baseline of authorized shares **and permissions** in association with the shared data" (emphasis added), as claimed by appellant. In addition, the mere disclosure in Meadway that index "updates [are] transmitted whenever the user connects to the central service" fails to disclose a technique "wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline" (emphasis added), as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #2: Claims 5, 19 and 33*

The Examiner has relied on Col. 3, lines 25-30 and 45-50 in Welch to make a prior art showing of appellant's claimed "pattern of activity [that] is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol." Appellant notes, however, that such excerpts from Welch only generally disclose "analyz[ing] logical connections and file transfers...by examining the information of layers 2,3, and 4" where "protocol control information 42 [is] available in layers 2, 3, 4 and 7 of a packet." Only generally examining protocol control information, however, does not meet appellant's claimed "pattern of activity", let alone "a pattern of activity [that] is defined in terms of network traffic...that uses a specific protocol" (emphasis added).

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that "the claim does not explicitly point out which protocol is being used, just that a specific protocol is being used" and "[t]herefore, any protocol would satisfy the limitation." Further, the Examiner asserts that "in Welch, the two peers that are transmitting files (Welch, col. 5, lines 60-67) must be following a specific protocol in order for successful communication" and "therefore, monitoring this file transfer would require monitoring a specific protocol." However, appellant asserts that Welch merely discloses that "[f]or each file transfer record 91, AME 81 notes the identity of the two

stations involved in the file transfer using peer A pointer field 91a and peer B pointer field 91b." Clearly, the mere disclosure of two stations involved in a file transfer completely fails to even suggest a "pattern of activity [that] is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #3: Claims 11, 25 and 39*

The Examiner has relied on the following excerpt from Welch to make a prior art showing of appellant's claimed technique "wherein the patterns of activity are local to a peer in the peer-to-peer network."

> "...a copy of the revised connection record 93 to the archive. This allows dynamic display of connection activity. Analysis of the packet complete, CME 83 branches to step 204.
>
> Thus, methods of monitoring both local connections and file transfers in a computer network have been described." (Col. 10, lines 5-10)

Appellant respectfully asserts that such excerpt merely discloses "monitoring...local connections and file transfers." Clearly, mere local connections do not meet appellant's claimed "patterns of activity [that] are local to a peer in the peer-to-peer network" (emphasis added).

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that "[appellant] does not provide any reasoning for this assertion" and "submits that by Welch disclosing monitoring file transfers from peer A to peer B (Welch, col. 5, lines 58-67) includes monitoring patterns of activity that are local to the peer." Appellant respectfully asserts that Welch merely discloses, in item 114 of Fig. 5, that if "this [is] an open file request" then item 116, of Fig. 5, "create[s] a record of this connection in database." Clearly, monitoring for open file requests between peer stations fails to even suggest a technique "wherein the patterns of activity are local to a peer in the peer-to-peer network" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #4: Claim 45*

The Examiner has relied on the following excerpt from Meadway to make a prior art showing of appellant's claimed technique "wherein a share configuration loop is executed to detect changes to shares and corresponding permissions, and take an action as a function of a type of the changes."

> "...agent program downloaded and installed by each peer system user. This agent program is described in detail in pending U.S. patent application Ser. Nos. 09/419,405, U.S. Pat. No. 6,516,337, and 09/575,971, filed May 23, 2000, by the same inventors which are hereby incorporated by reference. The indexing process on each system may be initiated manually or on a scheduled basis, with updates transmitted whenever the user connects to the central service.
>
> The agent is also responsible for transmitting copies of the requested file to the systems whose requests are waiting..." (Col. 2, lines 1-10)

Appellant respectfully asserts that the agent program disclosed in Meadway is simply associated with the indexing process where the index is of "the contents of the files" on peers (see Col. 2, lines 14-15). Simply nowhere in Meadway is there even any mention of a "share configuration loop [that] is executed to detect changes to shares and corresponding permissions, and take an action as a function of a type of the change," as claimed by appellant (emphasis added).

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that appellant's claimed technique "wherein a share configuration loop is executed to detect changes to shares and corresponding permissions, and take an action as a function of a type of the changes" reads "...take action as a function of a type of the change." Appellant respectfully disagrees. In addition, the Examiner has argued that "Meadway disclosed that when the central server receives an updated version of the client's index of shared data on a scheduled basis (Meadway, col. 2, lines 5-7), the central server performs updating the changes in the central server's index (Meadway, col. 4, lines 18-25)." However, appellant asserts that Meadway discloses "updates [which are] transmitted whenever the user connects to the central service" and that the "indexing

process on each system may be initiated manually or on a scheduled basis" (emphasis added). In addition, Meadway discloses that a "number of update servers 222 each receive updates from the agent programs and store the current version of the agent program for download and update of the local agent programs." Further, Meadway discloses that "[e]ach of the update servers 222 applies all index change transactions through a firewall/router 224 to the master index server 218." However, merely transmitting updates whenever the user connects to the central service, and having the update servers apply all index change transactions to the master index server, fails to even suggest a technique "wherein a share configuration loop is executed to detect changes to shares **and** corresponding permissions, and take an action as a function of a type of the changes" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #5: Claim 46*

The Examiner has again relied on Col. 2, lines 1-10 of Meadway to make a prior art showing of appellant's claimed technique "wherein the share configuration loop is executed dynamically." Appellant respectfully asserts that such excerpt along with the entire Meadway reference fail to meet appellant's claimed "share configuration loop," and thus also cannot meet the instant claim language further describing the claimed share configuration loop. Again, appellant respectfully asserts that the agent program disclosed in Meadway is merely associated with the indexing process where the index is of "the contents of the files" on peers (see Col. 2, lines 14-15). Simply nowhere in Meadway is there even any mention of a "share configuration loop [that] is executed dynamically," as claimed by appellant (emphasis added).

In the Examiner's Answer dated 08/27/2007, the Examiner argues that "[w]henever an agent sends an updated index to the central server, the central server updates its local index" which "does not require a user to update the local index." Appellant respectfully disagrees with the Examiner's assertions and asserts that Meadway merely discloses that "updates [are] transmitted whenever the user connects to the central service." Clearly, transmitting updates when the user

connects, fails to even suggest a technique "wherein the share configuration loop is executed dynamically" (emphasis added), as claimed by appellant. Also, appellant respectfully asserts that the mere disclosure that "[t]he master index server 218 also sends instructions to the Name Space/Directory Server 233 to dynamically determine which set of index servers 216 is to remain on-line to service search requests, and which set is to receive the updates" (emphasis added), fails to support the Examiner's assertion that "any functionality of the server [is] dynamic" (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #6: Claim 47*

The Examiner has again relied on Col. 2, lines 1-10 of Meadway to make a prior art showing of appellant's claimed technique "wherein the share configuration loop is executed on a schedule." Appellant respectfully asserts that such excerpt along with the entire Meadway reference fail to meet appellant's claimed "share configuration loop" and thus also cannot meet the instant claim language further describing the claimed share configuration loop. Again, appellant respectfully asserts that the agent program disclosed in Meadway is merely associated with the indexing process where the index is of "the contents of the files" on peers (see Col. 2, lines 14-15). Simply nowhere in Meadway is there even any mention of a "share configuration loop [that] is executed on a schedule," as claimed by appellant (emphasis added).

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that "Meadway disclosed the indexing process on each system may be set on a scheduled basis (Meadway, col. 2, lines 5-10)." Appellant asserts Meadway discloses that the "indexing process on each system may be initiated manually or on a scheduled basis" (emphasis added). However, merely initiating an indexing process on a scheduled basis fails to even suggest a "share configuration loop [that] is executed on a schedule" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #7: Claim 48*

The Examiner has again relied on Col. 2, lines 1-10 of Meadway to make a prior art showing of appellant's claimed technique "wherein the share configuration loop examines a current share configuration against a previously recorded shared configuration." Appellant respectfully asserts that such excerpt along with the entire Meadway reference fail to meet appellant's claimed "share configuration loop" and thus also cannot meet the instant claim language further describing the claimed share configuration loop. Again, appellant respectfully asserts that the agent program disclosed in Meadway is merely associated with the indexing process where the index is of "the contents of the files" on peers (see Col. 2, lines 14-15). Simply nowhere in Meadway is there even any mention of a "share configuration loop [that] examines a current share configuration against a previously recorded shared configuration," as claimed by appellant (emphasis added).

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that "Meadway disclosed when the central server receives an updated version of the client's index of shared data (Meadway, col. 2, lines 5-7); the central server performs updating the central server's local index (Meadway, col. 4, lines 18-25). However, appellant asserts that Meadway discloses that "the update servers store the digital signature of the agent program and also store the remote web hosts' last local index, which are utilized during the updating of the remote agent program and during updating the local index" (emphasis added). Appellant asserts that the mere disclosure that the update servers utilize the last local index during updating the local index fails to suggest a technique "wherein the share configuration loop examines a current share configuration against a previously recorded shared configuration" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #8: Claim 49*

The Examiner has yet again relied on Col. 2, lines 1-10 along with Col. 2 lines 35-41 in Meadway to make a prior art showing of appellant's claimed technique where "if the change includes an attempt to un-share a file or directory, the action includes a log entry." Appellant asserts that such excerpts do not teach any sort of "attempt to un-share a file or directory" as claimed by appellant, but instead only disclose indexing the contents of files and an "agent that reports to the central server the identities of files on the computer that will be provided if requested by others." In addition, such excerpts also fail to teach "a log entry" action if a change is made with respect to un-sharing a file or directory, in the manner claimed by appellant.

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that "any change in the peer's local index, regarding what files are shared or not shared by the peer, is included in the updated index that is sent to the central server, and the central server updates its local index (Meadway, col. 1, lines 45-50, col. 2, lines 1-10, 35-40)." However, appellant respectfully asserts that Meadway discloses that "[t]he indexing process on each system may be initiated manually or on a scheduled basis, with updates transmitted **whenever** the user connects to the central service" (emphasis added). In addition, Meadway discloses that "[t]he agent reports to the central server the identities of files on the computer that will be provided if requested by others." Clearly, the disclosure in Meadway of an indexing process that is initiated manually or on a schedule, where updates transmitted to the central service whenever the user connects, fails to even suggest "if the change includes an attempt to un-share a file or directory, the action includes a log entry" (emphasis added), as claimed by appellant. Further, the excerpts Meadway relied upon by the Examiner fail to disclose an "action includ[ing] a log entry" resulting from a "change includ[ing] an attempt to un-share a file or directory." Also, appellant asserts that the Examiner's statement that the "local index of the central server is a log of the files permitted for sharing by each peer" improperly equates an index with a log.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue #3:

The Examiner has rejected Claims 4, 7, 9, 10, 12-14, 18, 21, 23, 24, 26-28, 32, 35, 37, 38 and 40-44 under 35 U.S.C. 103(a) as being unpatentable over Welch, Jr. et al., U.S. Patent No. 5,862,335, in view of Meadway et al., U.S. Patent No. 6,675,205, in further view of Conklin et al., U.S. Patent No. 5,991,881.

*Group #1: Claims 4, 10, 12, 18, 24, 26, 32, 38 and 40-42*

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #2, Group #1.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #2: Claims 7, 21 and 35*

The Examiner has relied on the following excerpt from Conklin to make a prior art showing of appellant's claimed "pattern of activity [that] is defined in terms of network traffic in the peer-to-peer network having a foreign address."

> "**When a packet or accumulation of packets match a predefined intrusion profile** the Intrusion Detection function identifies the network traffic as a reportable activity **will construct a data structure which contains** a date/time stamp indicating the time of detection, **the source and destination Internet Protocol (IP) addresses**, an assigned message identifying the event detected. This data structure is passed to the Alert Notification function for processing. When a positive identification of a reportable activity occurs, the entire triggering packet(s) may be written to a log file created in the Evidence Logging function." (Col. 5, lines 25-35-emphasis added)

Appellant respectfully asserts that the above excerpt from Conklin only teaches that "[when] a packet or accumulation of packets match a predefined intrusion profile [then] a data structure [will be constructed] which contains...the source and destination...addresses" (see emphasized

excerpt above). Thus, the pattern of activity in Conklin is not taught to be "defined in terms of network traffic...having a foreign address," as claimed by appellant, but instead only general source and destination addresses are reported after the match is made.

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that "[s]ince Conklin identifies intrusions into the network from an external source, Conklin disclosed reporting patterns of activity that is defined in terms of network traffic having a foreign address." Appellant respectfully disagrees with the Examiner's interpretation and asserts that Conklin discloses "a system and method for network surveillance and detection of attempted intrusions, or intrusions, into the network and into computers connected to the network" (Abstract – emphasis added). In addition, Conklin discloses that "[w]hen a packet or accumulation of packets match a predefined intrusion profile the Intrusion Detection function identifies the network traffic as a reportable activity will construct a data structure which contains a date/time stamp indicating the time of detection, the source and destination Internet Protocol (IP) addresses..." (emphasis added). Appellant asserts that a data structure containing source and destination IP addresses fails to even suggest a "pattern of activity [that] is defined in terms of network traffic in the peer-to-peer network having a foreign address" (emphasis added), as claimed by appellant. In addition, appellant respectfully asserts that mere disclosure of a source IP address fails to support the Examiner's argument that "[t]he source of the intrusion has an address outside the network, hence foreign."

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #3: Claims 9, 23 and 37*

The Examiner has relied on Col. 5, lines 33-35 of Conklin, as excerpted above, to make a prior art showing of appellant's claimed technique "wherein the action comprises logging information about the particular pattern." However, appellant respectfully asserts that only "the entire triggering packet(s) [are] written to a log file" in Conklin (emphasis added), and not "information about the particular pattern," as claimed by appellant (emphasis added).

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that "if the packet is detected as being part of a particular pattern, and the entire packets is written to a log file (Conklin, col. 5, lines 33-36), then this must contain information regarding the particular pattern, since the packet is what caused the detection in the first place." Appellant respectfully disagrees with the Examiner's argument, and asserts that Conklin merely discloses that "[w]hen a positive identification of a reportable activity occurs, the entire triggering packet(s) may be written to a log file created in the Evidence Logging function" (emphasis added). Clearly, the mere disclosure of writing the entire triggering packet(s) to a log file fails to even suggest a technique "wherein the action comprises logging information about the particular pattern" (emphasis added), as claimed by appellant. Appellant asserts that Conklin suggests writing the triggering packet(s) to the log file, and not information about the particular pattern that caused the trigger.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #4: Claims 13, 27 and 43*

The Examiner has relied on Col. 4, lines 45-55 in Conklin to make a prior art showing of appellant's claimed "obtaining a set of rules specifying the patterns of activity and associated actions." Appellant notes, however, that the above excerpt in Conklin completely fails to even mention "a set of rules specifying the patterns of activity and associated actions," as claimed by appellant (emphasis added). In fact, even the Examiner, in his rejection, states that "Conklin disclosed obtaining pre-stored patterns of activity in a database," but fails to address any "associated actions" as in appellant's claim language.

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that 'the limitation, "associated actions" in its broadest reasonable interpretation, could simply mean an action describing the pattern of activity, hence the pattern of activity.' In addition, the Examiner has argued that "[o]ne of ordinary skill in the art would interpret patterns of activity to include associated actions since a pattern of activity would require actions." Appellant respectfully

disagrees with the Examiner's arguments and asserts that Conklin discloses that "[i]f the collected data matches the databases stored data, ... then the Network Surveillance System identifies the network data as a reportable activity and the Network Surveillance System components ... are activated and a data channel is opened between the Network Observation function ... and the Evidence Logging function" (emphasis added). Clearly, Conklin's actions of identifying, activating, and opening a data channel when collected data matches the database's stored data fails to meet and even *teaches away* from the need for "a set of rules specifying the patterns of activity and associated actions" (emphasis added), as claimed by appellant, since the actions are already defined for all data matches.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

*Group #5: Claims 14, 28 and 44*

The Examiner has relied on the following excerpt from Conklin to make a prior art showing of appellant's claimed "refreshing the set of rules when the set of rules changes."

> "the Intrusion Detection function examines the data in comparison to a series of predefined or learned patterns which are pre-stored or developed from data received from the network.
>
> In the preferred embodiment, the network data is compared to a database of known patterns." (Col. 4, lines 48-52)

Appellant respectfully asserts that the above excerpt merely discloses comparing "the data...to a series of predefined or learned patterns which are pre-stored." However, nowhere in such excerpt or the entire Conklin reference is there any suggestion of "refreshing the set of rules when the set of rules changes," as claimed by appellant (emphasis added).

In the Examiner's Answer dated 08/27/2007, the Examiner has argued that Conklin's disclosure on Col. 4, lines 45-50 that "Intrusion Detection may incorporate algorithms or patterns to detect attempted intrusions or intrusions on the network (Conklin, col. 4, lines 45-50), means that algorithms may be added to the Intrusion Detection system, thereby refreshing sets of rules to

follow." Appellant respectfully disagrees with the Examiner's interpretation and asserts that Conklin merely discloses that "Intrusion Detection may incorporate algorithms or patterns to detect attempted intrusions or intrusions on the network." Simply disclosing that Intrusion Detection incorporates algorithms or patterns fails to even suggest "refreshing the set of rules when the set of rules changes" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P344).

Respectfully submitted,

By: /KEVINZILKA/ Date: September 27, 2007
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660